Notice of Data Breach

We are writing to make you aware of a recent privacy issue at Catholic Charities of San Diego ("Catholic Charities"). We take the privacy of our clients very seriously and understand that your personal information is important to you. This notice is applicable to clients of Catholic Charities' homeless services division.

What Happened

Catholic Charities was recently the victim of a ransomware attack. The attack was discovered on March 30, 2020. While we do not know for certain, presumably the ransomware was deployed sometime between the close of business on Friday, March 27, 2020 and early morning on Monday, March 30, 2020. Upon discovering the attack, we immediately shut down our entire system and began investigating. We notified the FBI and retained a forensic firm to conduct a thorough investigation. While we initially tried to recover the data from our backups, we were unable to do so. Ultimately, we ended up paying the attacker and recovering all of our data. We do not have any evidence that the attacker or anyone else has misused any of the data subject to the attack. However, we do know that an unauthorized person or persons had access to the data for a short period of time. Therefore, we are notifying you of the incident.

What Information Was Involved

The information involved in the attack included the following:

1) Name
2) Date of Birth
3) Social security number
4) Criminal history (if applicable)
5) Case notes, including public benefits information
6) Copies of identification cards (if given to us)
7) Medical information

What We Did and What We Are Doing

As soon as Catholic Charities discovered the ransomware attack, we immediately began investigating and gathering information. The entire system was shut down while we figured out what happened and could confirm that the ransomware was no longer active. Relevant passwords were immediately changed and the compromised accounts were removed from the system. After paying the ransom, we confirmed that all of our data was recovered and restored. Monitoring and anti-crypto software was deployed. The environment targeted in the attack was retired. We are in the process of moving our backups to a cloud-based system, which will help protect against this type of incident in the future. Finally, we filed a report with the FBI and are working with local law enforcement to provide it with information to assist in its investigation. We will continue to cooperate with any investigations into this matter.

We take our responsibility to safeguard your personal information seriously. We are sorry this happened. In the interest of protecting our clients, we are offering identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts to enroll in free MyIDCare services by calling 800-939-4170. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is August 29, 2020

We encourage you to take full advantage of this service offering and reach out to Catholic Charities with any questions and concerns.

There are additional actions you can consider taking to reduce the risk of identity theft or fraud on your account(s). Please refer to the enclosed Recommended Steps document for more information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document.

Please call 800-939-4170 for assistance with any additional questions you may have about enrolling in MyIDCare services.

If you have any questions about the underlying incident, please feel free to call 833-579-1101.

Sincerely,

Appaswamy "Vino" Pajanor
Chief Executive Officer
Catholic Charities, Archdiocese of San Diego

(Enclosure)

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

2. Telephone. Contact MyIDCare at 800-939-4170 to enroll and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.